UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE PERSON OF MARK E. BUTLER AND THE RESIDENCE LOCATED AT 15 TURGEON'S LANE, APARTMENT B IN SOMERSWORTH, NEW HAMPSHIRE	))))))	No. 1:21-MJ-268-01-AJ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Adam Rayho, a Task Force Officer with the United States Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), being duly sworn, depose and state as follows:

INTRODUCTION

1. I am investigating the activities of Mark E. Butler ("BUTLER"), who resides at 15 Turgeon's Lane, Apartment B, in Somersworth, New Hampshire ("SUBJECT PREMISES"). As will be shown below, there is probable cause to believe that BUTLER has committed the offenses of distribution, receipt, advertisement, and possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2), 2252A(a)(3)(B), and 2252A(a)(5)(B). I submit this affidavit in support of a warrant under Rule 41 of the Federal Rules of Criminal Procedure to seize and search the person of Mark E. BUTLER and the SUBJECT PREMISES, which are further described in Attachment A and incorporated herein by reference, for evidence, fruits, and instrumentalities of the forgoing criminal violations. I specifically request authority to search BUTLER's person and the entire SUBJECT PREMISES for any computer and computer media located therein where the items specified in Attachment B, incorporated herein by reference, may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of criminal activity.

2. This affidavit is based in part on information that I learned from discussions with other law enforcement officers and on my own investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of 18 U.S.C. §§ 2252A(a)(2), 2252A(a)(3)(B), and 2252A(a)(5)(B), are presently located on BUTLER's person and the SUBJECT PREMISES.

AGENT BACKGROUND

3. I am a detective with the Nashua, New Hampshire Police Department, and a deputized task force officer (TFO) for HSI. I became a certified police officer in the State of New Hampshire in May 2014 after graduating from the 164th New Hampshire Police Standards and Training Academy. I have also completed HSI's Task Force Officer Course. I hold a bachelor's degree in criminal justice, with a minor in computer science and victimology, from Endicott College.

4. Since November 2019, I have been assigned to the Special Investigations Division as a member to the New Hampshire Internet Crimes Against Children (ICAC) Task Force, which includes numerous federal, state, and local law enforcement agencies conducting proactive and reactive investigations involving online child exploitation. As a TFO, I am authorized to investigate violations of federal laws and to execute warrants issued under the authority of the United States. Specifically, as a TFO and a member of the ICAC, I investigate criminal violations related to online sexual exploitation of children. I have received training in the areas of child sexual exploitation including, but not limited to, possession, distribution, receipt, and production of child pornography, and interstate travel with intent to engage in criminal sexual

activity, by attending training hosted by the ICAC involving online undercover chat investigations and interview/interrogation. I have also participated in numerous online trainings hosted by the Federal Bureau of Investigation Child Exploitation and Human Trafficking Task Force Online Covert Employee Development Series. These trainings focused on live stream investigations and using undercover personas on various social media applications for proactive investigations. I have personally conducted numerous online undercover investigations using social media applications such as KIK messenger, Grindr, WhatsApp, Whisper, and MeetMe. In addition, I have completed the Cellebrite Certified Operator and Cellebrite Certified Physical Analyst course in mobile forensics. In the course of investigating crimes related to the sexual exploitation of children, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have been involved in numerous online child sexual exploitation investigations and am very familiar with the tactics used by child pornography offenders who collect child pornographic material and those who seek to exploit children.

5. In addition, over the course of this investigation, I have conferred with other investigators who have conducted numerous investigations and executed numerous search and arrest warrants which involved child exploitation and/or child pornography offenses.

STATUTORY AUTHORITY

6. This application is part of an investigation into Mark E. Butler for the alleged knowing distribution, receipt, advertisement, and possession of child pornography. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving and distributing any child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means,

including by computer. 18 U.S.C. § 2252A(a)(3)(B) prohibits a person from knowingly advertising using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any material or purported material in a manner that reflects the belief that, or that is intended to cause another to believe, that the material or purported material is, or contains a visual depiction of an actual minor engaging in sexually explicit conduct. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

CHARACTERISTICS OF CHILD PORNOGRAPHY OFFENDERS

7. Based upon my knowledge, experience, and training in child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to many individuals involved in such crimes:

a. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes,

books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child-pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home, or in some other secure location.

d. Likewise, those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area.

e. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes also may correspond with others to share information and materials.

BACKGROUND ON GRINDR, WHATSAPP, AND ZOOM

8. Grindr is a location-based social networking and online dating application for gay, bi, trans, and queer people available on iOS and Android devices. The application is owned by Grindr LLC, and headquartered in West Hollywood, California. In order to use Grindr individuals must download the application and sign up using an email address or phone number. During the registration process the user is not required to validate the email address or phone number used to sign up, thus neither the email address or phone number actually have to belong

to them or be a legitimate email address/phone number. Once the user registers the account, the only information they are required to provide is a date of birth, which is again not verified and can be changed when setting up their profile. The minimum age allowed to create and be displayed in a Grindr account is 18-years-old. Once the account is created, users have the option to display their age, write an "about me" section, and indicate other demographic, biographical, and sexual information. Furthermore, users may opt to, but are not required to, create a username which is not unique and can be the exactly the same for different individuals. Individuals can find other individuals to speak with on Grindr based off their current location or can search for individuals within a certain area. Further advanced features are available on Grindr with a paid subscription.

9. WhatsApp Messenger, or simply WhatsApp, is a freeware, cross-platform centralized instant messaging and voice-over-IP service. The application is owned by Facebook, Inc., and headquartered in Menlo Park, California. WhatsApp allows users to send text messages and voice messages, make voice and video calls, and share images, documents, user locations, and other content. In order to create a WhatsApp account, users must provide a phone number and are sent a text message which requires the user to verify the phone number. Once the account is created, user can, but are not required to, create a username, add a picture, and enter information about themselves. Messages between WhatsApp users are encrypted at a user-level, meaning Facebook, Inc., does not have access to the messages and they are only available on the user's device. Furthermore, there are different settings users can apply to the messages which include having them delete after a certain amount of time.

10. Zoom Meetings, commonly referred to as Zoom, is a proprietary video teleconferencing software program developed by Zoom Video Communications Inc., and is

headquartered in San Jose, California. The free plan allows up to 100 concurrent participants, with a 40-minute time restriction. The service is available on mobile (Android & iOS) devices along with tablets, laptops, and desktops. In order to host a meeting, users must register an account using their email address. In order to join a meeting, users must obtain the meeting link and password. Once in a meeting, users have multiple options on if they are seen or heard, such as choosing to display their video or mute themselves. Additionally, users can record the meetings they are a part of.

PROBABLE CAUSE

Initial Investigation:

11. On March 24, 2021, Officer Nicole Lefebvre of the Somersworth, New Hampshire Police Department ("SPD") took a report from Individual A, a 17-year-old male, regarding an individual using the Grindr username "NH_Leather," who sought to engage in sexual activity with Individual A. Individual A's profile listed his age at 18; however, during their chats, BUTLER questioned Individual A about his age. Specifically, BUTLER stated, "More often than not profiles on here that list them selves as 18 are typically 15 16 or 17. Are you under 18 or 18? And again even if you were to say 15 it does not matter :-)". At first, Individual A informed BUTLER that he was 18 years old, which BUTLER advised was too old for him. Individual A later told BUTLER, "Ok I'm actually not 18 for like 5 days lmai". In response, BUTLER wrote, "LOL. Well I'm kind of thinking that my lips need to be wrapped around your dick". Thereafter, BUTLER sent Individual A images, including an image law enforcement believed to be a nude photo of BUTLER holding his erect penis. In addition, BUTLER later invited Individual A to his residence of "15 Turgeon's Lane, Apartment B, Somersworth, New Hampshire". Furthermore, BUTLER told Individual A that a 14-year-old

neighbor's son sneaks over his residence through BUTLER's sliding door and BUTLER reiterated that age is not a factor. During the conversation with Individual A, BUTLER provided his address as 15 Turgeon's Lane, Apartment B, Somersworth, New Hampshire. With the consent of Individual A and his parent, law enforcement attempted to extract his cell phone. Due to a technical issue, law enforcement took screenshots of the relevant chats and images exchanged between BUTLER and Individual A.

12. Officer Lefebvre reviewed some of the pictures "NH_Leather" sent to Individual A, and subsequently identified the user of the Grindr username "NH_Leather" as Mark BUTLER of Somersworth, New Hampshire.

13. On March 26, 2021, New Hampshire State Police Trooper Hawley Rae became involved in this investigation and reviewed screen shots of the conversation between BUTLER and Individual A. Trooper Rae noted four sexually suggestive images that BUTLER shared with Individual A. The images showed BUTLER naked on a bed with his legs spread, his testicles and penis displayed; a flaccid penis; an erect penis; and an image of BUTLER naked in a pool. BUTLER also sent several selfies amongst the pictures of his penis to Individual A. In the chats, BUTLER asked Individual A, "can you send me some pictures of you or at least your dick". Individual A did not send any sexually explicit images to BUTLER.

14. Based on her review of the relevant chats and images, Trooper Rae obtained a search warrant for Individual A's Grindr account. Grindr's response to the search warrant was limited to Individual A's profile ID, account creation date, and display name. Grindr does not retain any chats or images shared by its users. Trooper Rae was unable to determine the email address used by BUTLER to create the Grindr account for username "NH_Leather" and no further legal process was directed to Grindr.

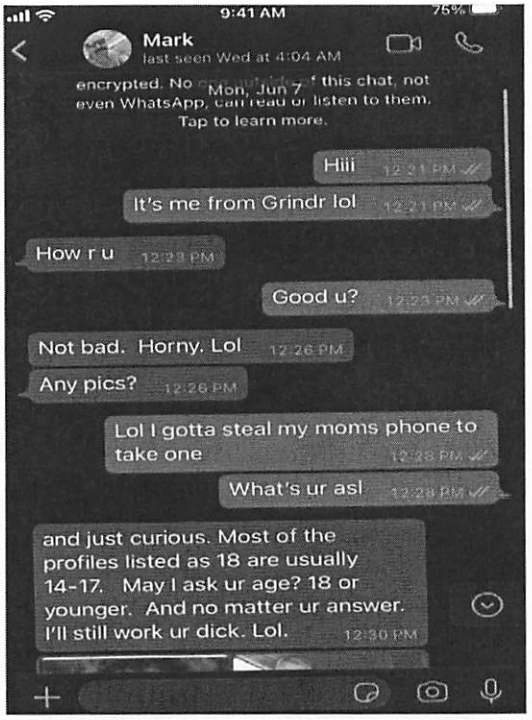
Undercover Investigation:

15. On May 12, 2021, New Hampshire State Trooper Sergeant Tamara Hester contacted me regarding the investigation into BUTLER and asked that I attempt to further the investigation into Grindr username "NH_Leather".

16. In order to investigate online child exploitation matters, I maintain several undercover profiles across various social media platforms, including Grindr and WhatsApp. Over the course this investigation, I used the undercover persona of a 13-year-old male on Grindr and WhatsApp and the undercover persona of a 35-year-old male on WhatsApp.

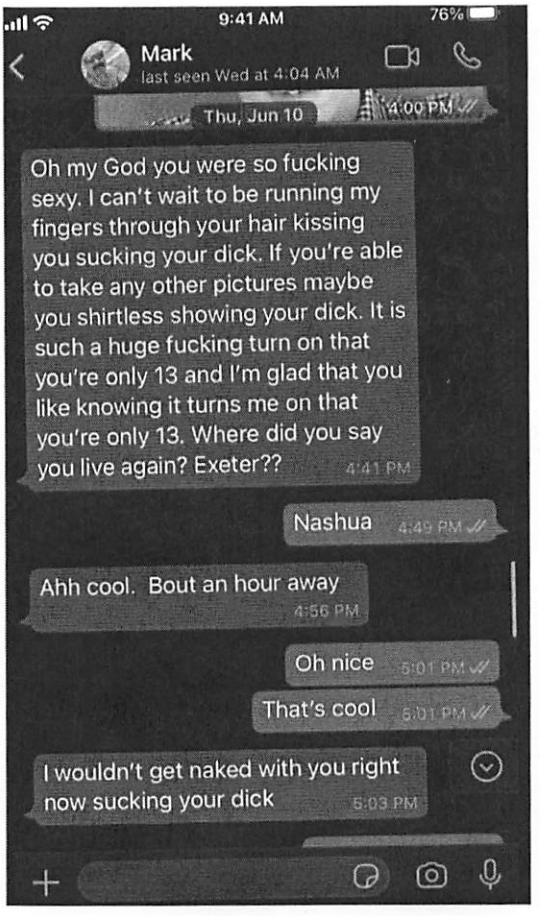
17. On June 3, 2021, using the 13-year-old undercover Grindr profile, I observed that Grindr user "NH_Leather" was active. The profile displayed a picture of a male I later identified as BUTLER. I proceeded to message Grindr user "NH_Leather". During our initial conversation I made references to being a child by stating, "Nm I'm bored just chillin. My mom isn't home from work yet lol" and "Lmao. Umm not Rn gotta steal my moms phone n take 1".

18. From June 3, 2021, through September 13, 2021, I continued to communicate with BUTLER using the undercover 13-year-old persona during which time BUTLER reiterated his sexual interest in minors, including in the chats excerpted below [his statements are in the dark gray chat boxes]:


9:41 AM
75%
Mark
last seen Wed at 4:04 AM
encrypted. No
even WhatsApp,
Tap to learn more.
Mon, Jun 7
Hiii
It's me from Grindr lol
How r u
Good u?
Not bad. Horny. Lol
Any pics?
Lol I gotta steal my moms phone to take one
What's ur asl
and just curious. Most of the profiles listed as 18 are usually 14-17. May I ask ur age? 18 or younger. And no matter ur answer. I'll still work ur dick. Lol.


9:41 AM
75%
Mark
last seen Wed at 4:04 AM
12:32 PM Mon, Jun 7
Lol I'm 13
Promise u won't report me?
I totally promise and thank you for feeling comfortable and safe enough to be honest with me
12:40 PM
I want ur cock
12:41 PM


9:41 AM
75%
Mark
last seen Wed at 4:04 AM
Mon, Jun 7
Nashua
Cool. I hope it's ok I'm very turned on that u r 13
2:04 PM
Really?
R u there?
Am sorry had errands ha dtondo. Just got back to hotel
7:06 PM
And fuuuck yes. I love that 14
13
7:06 PM
My mom is home I'll message u tom
Tue, Jun 8
Hiii


9:41 AM
76%
Mark
last seen Wed at 4:04 AM
Thu, Jun 10
4:00 PM
Oh my God you were so fucking sexy. I can't wait to be running my fingers through your hair kissing you sucking your dick. If you're able to take any other pictures maybe you shirtless showing your dick. It is such a huge fucking turn on that you're only 13 and I'm glad that you like knowing it turns me on that you're only 13. Where did you say you live again? Exeter??
4:41 PM
Nashua
Ahh cool. Bout an hour away
4:56 PM
Oh nice
That's cool
I wouldn't get naked with you right now sucking your dick
5:03 PM

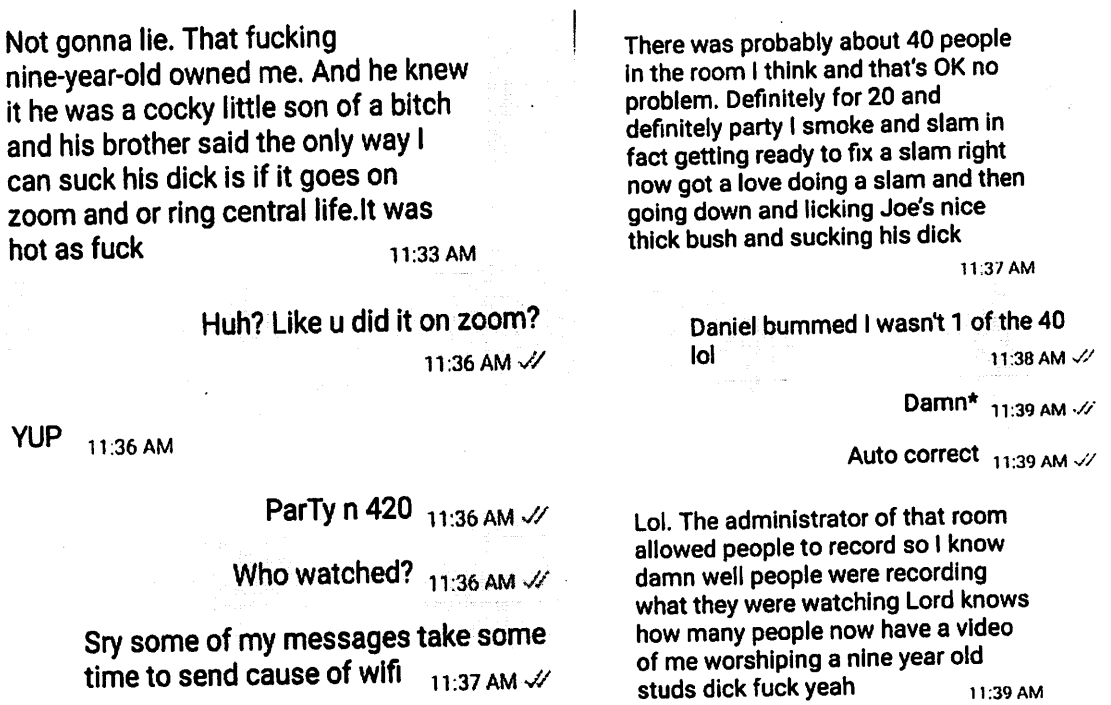
19. On September 13, 2021, over WhatsApp, to my 13-year-old persona, BUTLER asked if I was still using Grindr and talking to any other adults. In response, I advised that I was speaking with one other adult who knew I was 13. BUTLER then told me to provide the other adult his Grinder username and tell him that BUTLER liked that I was 13 years old. BUTLER later instructed me to give his WhatsApp number, (617) 480-4252, to the other adult.

20. On September 22, 2021, I contacted BUTLER over his WhatsApp number using the undercover 35-year-old persona. BUTLER identified himself as "Mark" and stated, "Have you had the pleasure of getting to suck on that 13 year old stud dick". BUTLER then stated, "He [13-year-old persona] sent me an audio clip because I told him I wanted to hear his voice. But I was also to help verify that he actually is 13 as opposed to an adult undercover. And it was crystal clear that that was a young boy's voice."

21. As our conversation progressed, on September 23, 2021, BUTLER informed me that he had met a 16-year-old on Grindr who "plays" with his 9-year-old brother and "I got to enjoy my time with both of them". I asked Butler how the 9-year-old was and he responded, "It's fucking amazing. Let me send you a quick hard video of him that he sent me". Butler sent the undercover 35-year-old persona a one-minute video of a prepubescent male. In the video, the prepubescent male removed his clothing until he was fully nude. Once nude, the prepubescent male began to masturbate his penis with both hands. As the video continued, the prepubescent male moved closer to the camera while holding his penis in one hand and using his other hand to touch the tip of his penis. In describing the child as a prepubescent male, I note that he did not have any pubic hair and his body structure and facial features appear consistent with a 9-year-old child. After receiving this video from BUTLER, I asked him, "That's the 9 or 16 yro" and he

responded, "Believe it or not that's the nine year old the kid knows what he's good and he loves showing off and believe me I loved worshiping his dick".

22. After BULTER sent the 1-minute video to the undercover 35-year-old persona, we continued to discuss his sexual interest in prepubescent boys. In the following excerpts from our discussion, BULTER [his statements are in the white chat boxes] provided details about his alleged sexual encounter with the 9-year-old boy over the Zoom platform:



Other Investigative Information:

23. In most online child exploitation cases, investigators are able to use legal process to determine the physical location of the target offenders through I.P. addresses from the applications they use to communicate with others. Because BUTLER used Grindr and WhatsApp to communicate with Individual A as well as the undercover personas, investigators have been unable to identify any I.P. addresses associated with his use of Grindr and WhatsApp during the relevant times. At this time, I do not know the email in which BUTLER used to create

his Grindr account and I unable to serve Grindr with legal process to determine if they retain I.P. addresses for his account(s). With respect to WhatsApp, based on my prior experience, I know that WhatsApp retains only the first and last I.P. address used by its account holders. Moreover, because WhatsApp is primarily a mobile-based application, the I.P. address may only associate the account with a mobile provider and such information may have limited value in identifying a target user's specific location at any given time.

24. Based on my review of law enforcement databases, BUTLER does not currently have an active driver's license in New Hampshire. During undercover conversations I had with BUTLER using both the adult and child personas, BUTLER advised that he lived in Somersworth, New Hampshire, and he explained that he is unable to drive due to an eye injury. Based on the photographs that BUTLER shared of himself during the undercover chats, I note that BUTLER was often depicted wearing an eye patch. In addition, I have reviewed images obtained from the Somersworth Police Department of BUTLER from prior arrests. By comparing the arrest photographs of BUTLER with certain images shared during the undercover operations, I believe the same person was depicted.

25. On September 29, 2021, HSI Special Agent Shawn Serra and I conducted a canvass of 15 Turgeon's Lane, Somersworth, New Hampshire using the ruse of an immigration overstay. 15 Turgeon's Lane is a multi-unit, two-story apartment building located at the end of the street. While facing the building from the street, three apartments are visible (apartments E, C, and B). BUTLER's residence, Apartment B, is located on the bottom right corner and has a red screen door along with the letter "B" next to the front door. During this canvass we first spoke with a resident of apartment C, whose identity is known to law enforcement but will be referred to as Neighbor A. Neighbor A advised that he and his family have lived in apartment C

for several years. When asked about his neighbors, Neighbor A informed us that a male named "Mark" and his mother have lived in apartment B for several years. Special Agent Serra and I next knocked on the door to Apartment B and made contact with BUTLER, whom I recognized from the Somersworth Police Department photographs and images he shared during the undercover chats. BUTLER identified himself as "Mark Butler," and he advised that he lived at the apartment with his mother for approximately four years. BUTLER also identified his phone number as (617) 480-4252, which matched the number he provided to both undercover personas.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

26. As described above and in Attachment B, this application seeks permission to search for records that might be found on BUTLER's person and/or the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a cell phone, a computer's hard drive, or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

27. I submit that if a computer, cell phone, or other storage medium is found on BUTLER's person and/or the SUBJECT PREMISES, there is probable cause to believe relevant evidence will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer/cell phone/other electronic storage media, the data

contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, the operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or "cache."

e. I am also aware, through training and experience, that digital storage devices have become interconnected, making it easy for even casual users of technology to transfer or copy images from one device to another, or to maintain duplicate copies on more than one device or storage medium. In fact, many devices such as smartphones can be set to automatically back up their contents to alternate storage facilities, such as laptop or desktop computers, another phone, photo-sharing websites, and cloud storage providers.

f. I am aware that the contents of smart phones can be synched with or backed up to other digital devices in a variety of ways. Smartphones can be connected through cables to other

devices, such as laptop computers, for data transfer. Smartphones can also connect to other devices and transfer photos or documents wirelessly through technology such as Bluetooth. Data can also be sent from the phone to an email account via the Internet, and subsequently downloaded from the Internet to a different device (such as a tablet, game system, or computer) for storage. In addition, many smartphones utilize "cloud" storage. Cellular telephones can be set to automatically back up their contents to user accounts hosted on servers of various cloud storage providers. Users can also opt to perform a back-up manually, on an as-needed basis. I am aware that some smartphones also back up their contents automatically to devices such as laptop computers. Additionally, cellular telephones can exchange data between two differing cellular communications devices and other types of electronic and media storage devices via Bluetooth or Wi-Fi, regardless of the type of operating system or platform being utilized to operate each of the electronic devices. In addition, media cards which contain many forms of data can be interchanged between multiple types of electronic devices, including but not limited to, different cellular telephones.

28. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers/cell phone/other electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer/cell phone/other electronic storage media on BUTLER's person and/or in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a

paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and

passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

29. Based on my training and experience I know that much of the media referenced above, which may contain contraband, fruits and evidence of crime, is by its very nature portable. This includes as example but is not limited to extremely compact storage devices such as thumb drives, laptop computers, and smart phones. In my training and experience, I know it is not uncommon for individuals to keep such media in multiple locations within their premises, including in outbuildings and motor vehicles, and/or on their person.

30. Searching storage media for the evidence described in the attachment may require a range of data analysis techniques. In most cases, a thorough search for information stored in storage media often requires agents to seize most or all electronic storage media and later review the media consistent with the warrant. In lieu of seizure, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the

warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files is evidence or instrumentalities of a crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

31. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when officers executing the warrant conclude that it would be impractical to review the hardware, media, or peripherals on-site, the warrant I am applying for would permit officers either to seize or to image-copy those items that reasonably appear to contain some or all of the evidence described in the warrant, and then later review the seized items or image copies consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

32. This warrant seeks authorization for law enforcement to compel Mark E. Butler (BULTER) to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. Grounds for this request follow.

33. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

34. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

35. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

36. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera

detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

37. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

38. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

39. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked fora certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped

with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

40. In light of the foregoing, and with respect to (1) any device found on the person of Mark E. Butler (BUTLER), or (2) any device at/in SUBJECT PREMISES reasonably believed to be owned, used, or accessed by BUTLER, law enforcement personnel seek authorization, during execution of this search warrant, to: (1) press or swipe the fingers (including thumbs) of BUTLER to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of BUTLER and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face of BUTLER and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

41. The proposed warrant does not authorize law enforcement to compel that an individual present at the SUBJECT PRESMISES state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel an individual present at the SUBJECT PRESMISES to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

42. Based on the foregoing, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the crimes of distribution, receipt, advertisement, and possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2), 2252A(a)(3)(B), and 2252A(a)(5)(B) may be located on the person of Mark E. BUTLER and the SUBJECT PREMISES. I therefore seek a warrant to search the person of Mark E. BUTLER and

the SUBJECT PREMISES, as further described in Attachment A, and to seize and search the items described in Attachment B.

43. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later identified by a computer forensic examiner.

Dated: October 7, 2021

Respectfully Submitted,

/s/ Adam Rayho
Adam Rayho
Task Force Officer
Homeland Security Investigations

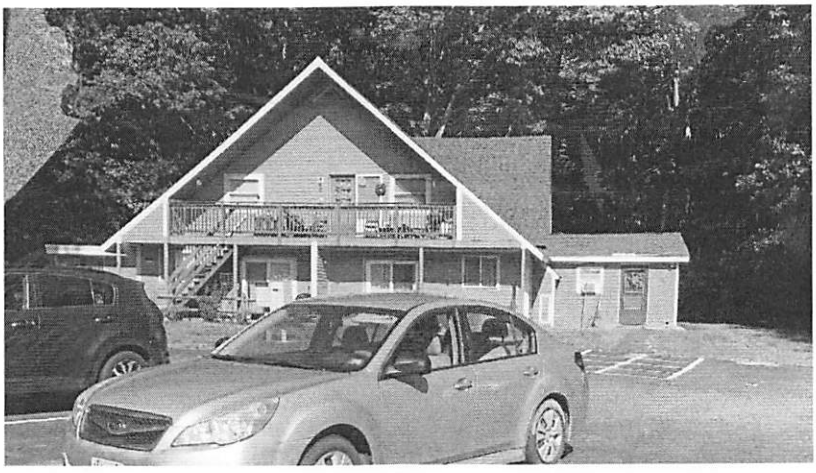
The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Andrea K. Johnstone
Honorable Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire
Dated: October 7, 2021

ATTACHMENT A

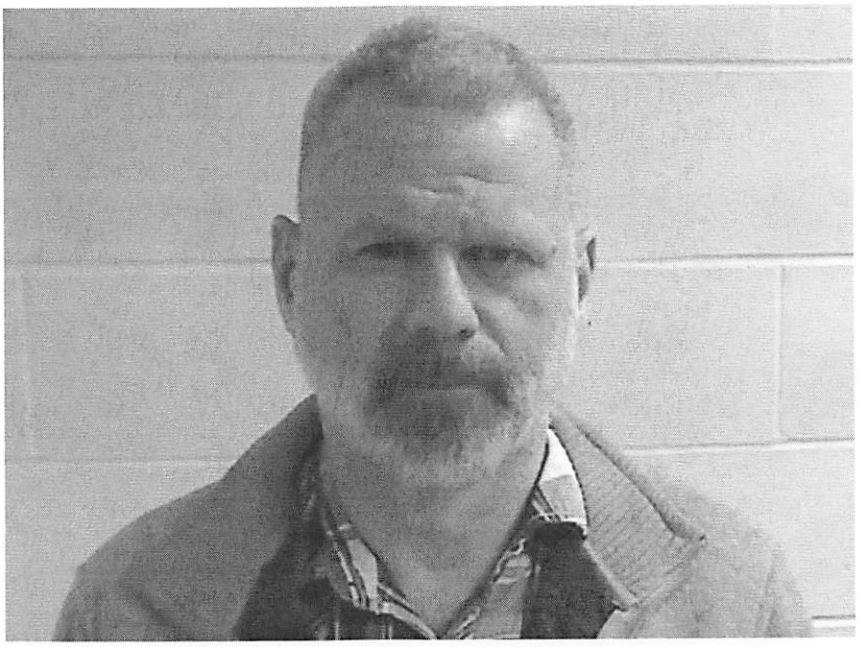
PREMISES TO BE SEARCHED

(1) The residential property located at 15 Turgeon's Lane, Apartment B, Somersworth, New Hampshire, which is a multi-family residence. Apartment B is located on the bottom right corner of the building when facing it, and is identified by a red screen door along with the letter "B" to the right of the door. The apartment building and apartment B are depicted in the following photographs:



Attachment A (continued)

(2) The person of Mark E. Butler, who is identified in the following photograph from 2019:



ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252A(a)(2), 2252A(a)(3)(B), and 2252A(a)(5)(B) (hereinafter, "SUBJECT OFFENSES"), in any form wherever they may be stored or found on the person of Mark E. Butler (BUTLER) and/or in the SUBJECT PREMISES, including:

1. Any cell phone, computer, computer hard drive, electronic media, or other physical object upon which electronic data can be recorded (hereinafter, "COMPUTER") that were or may have been used by BUTLER as a means to commit the SUBJECT OFFENSES;
2. Records and information relating to images or videos of suspected child pornography and visual depictions of minors engaged in sexually explicit conduct;
3. Records or information pertaining to an interest in child pornography;
4. Records and information relating to communications between individuals about child pornography;
5. Records and information relating to the existence of sites on the internet that contain child pornography or that cater to those with an interest in child pornography;
6. Records and information relating to membership in online groups, clubs, or services that provide or make accessible child pornography to members;
7. Records and information relating to any e-mail accounts used to view, access, trade or distribute child pornography;

8. Records or information pertaining to the receipt/distribution/possession/advertisement of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
9. Records or information pertaining to use of the applications WhatsApp and Grindr;
10. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
11. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software and evidence of the lack of such malicious software;
12. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
13. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
14. Evidence of the times the COMPUTER was used;
15. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
16. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

17. Records and things evidencing the use of the internet, including routers, modems, and network equipment used to connect computers to the internet;
18. Records of Internet Protocol addresses used;
19. Records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

DEVICE UNLOCK:

During the execution of the search of the property described in Attachment A, and with respect to (1) any device on Mark E. Butler's person, or (2) any device at/on the SUBJECT PREMISES reasonably believed to be owned, used, or accessed by Mark E. Butler, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of Mark E. Butler to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of Mark E. Butler and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face of that Mark E. Butler and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

DEFINITIONS:

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

As used above, the term "COMPUTER" includes but is not limited to any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile "smart" telephones, tablets, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, thumb drives, flash drives, Micro SD cards, SD cards, CDs, DVDs, tape drives and tapes, optical storage devices, zip drives and zip disk media, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, fax machines, digital cameras, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, routers, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or)signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).